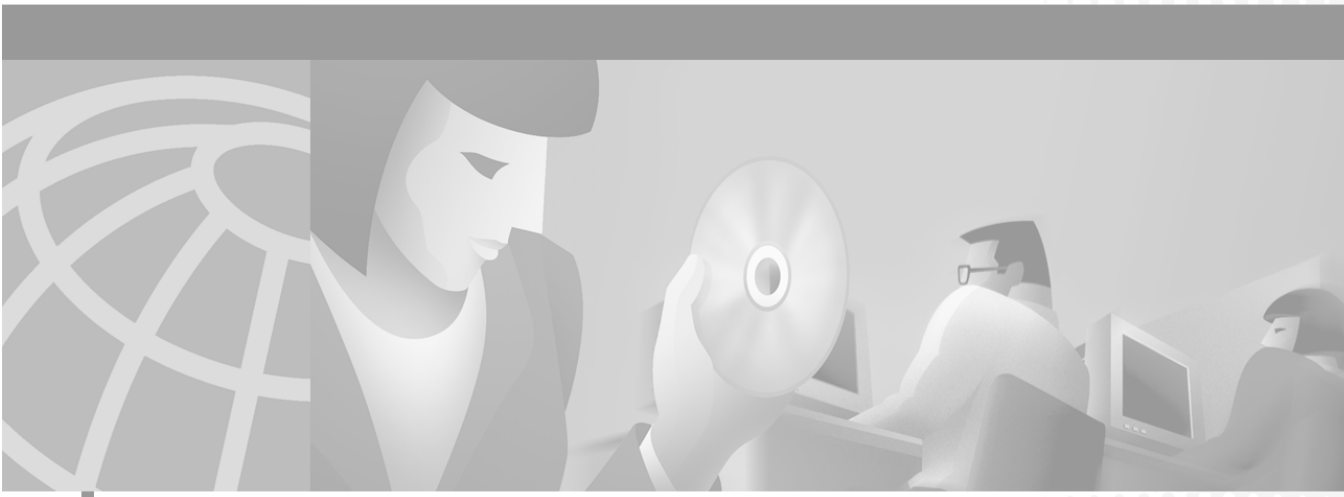


# Cisco VPN 5000 Client User Guide for Mac OS X

Version 5.2.x

March 2002

**Corporate Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-1446-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

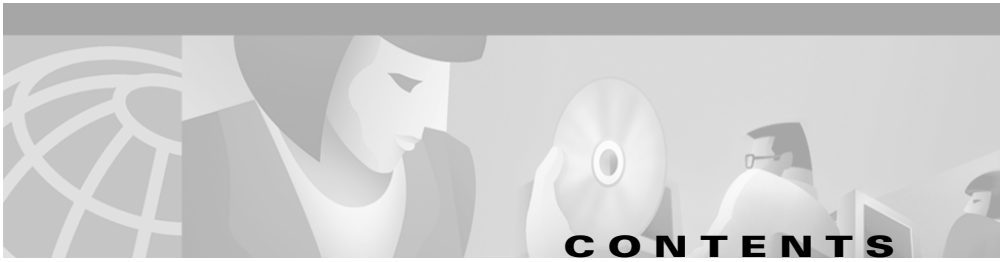
NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Fast Step, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0201R)

Copyright ©2002, Cisco Systems, Inc.
All rights reserved.



# CONTENTS


**About This Guide** **vii**

Contents **vii**

Obtaining Documentation **viii**

World Wide Web **viii**

Documentation CD-ROM **viii**

Ordering Documentation **viii**

Documentation Feedback **ix**

Obtaining Technical Assistance **ix**

Cisco.com **ix**

Technical Assistance Center **x**

Contacting TAC by Using the Cisco TAC Website **x**

Contacting TAC by Telephone **xi**

CHAPTER 1 **Introduction to the Cisco VPN 5000 Client** **1-1**

Features **1-1**

CHAPTER 2 **Installing the Cisco VPN 5000 Client** **2-1**

Contents **2-1**

Uninstalling the VPN Client for Mac OS X **2-1**

System Requirements **2-2**

Installing the Software **2-2**

CHAPTER 3 **Running the Cisco VPN 5000 Client** **3-1**

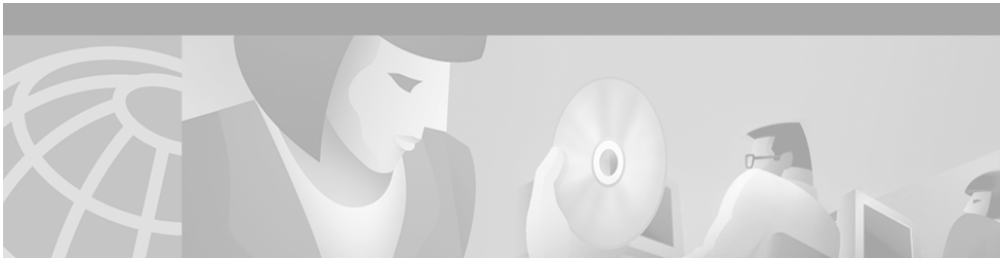
Contents **3-1**

Setting Up a Login **3-1**
Setting Up Digital Certificates **3-4**
Manual Certificates **3-4**
User Certificates **3-5**
Requesting Certificates from a Certificate Authority **3-7**
Connecting to the VPN Concentrator **3-8**
Connecting After Startup and Login **3-8**
Disconnecting the VPN Client **3-9**
Configuration File Description **3-9**

CHAPTER 4 **Cisco VPN 5000 Client User Interface 4-1**
Contents **4-1**
VPN Client Window **4-1**
Configurations Tab **4-2**
Network Interface **4-3**
Advanced Configuration Properties Dialog Box **4-4**
Login Properties Dialog Box **4-5**
Advanced Login Properties Dialog Box **4-8**
Logging Tab **4-9**
General Tab **4-11**
Certificates Tab **4-12**
Request Root Certificate Dialog Box **4-14**
Request User Certificate Dialog Box **4-15**
Digital Certificate Information Window **4-16**
About Tab **4-19**
Help Tab **4-20**
Security Prompts **4-20**
VPN Encryption Password **4-21**
Prompt for Secret **4-21**

RADIUS Login **4-22**
SecurID Challenge **4-24**
Changing the SecurID Passcode **4-26**
File Menu **4-26**

APPENDIX A **Configuration File Keywords A-1**
VPN Partner Aliases **A-1**
VPN User **A-2**
VPN General Section **A-4**
VPN Root Cert **A-4**
Example Configuration File **A-5**



# About This Guide

This guide provides users and administrators with information about the Cisco VPN 5000 Client software for the Mac OS X operating system.

## Contents

This guide contains the following chapters and appendixes:

- Chapter 1, “Introduction to the Cisco VPN 5000 Client.” This chapter describes how the VPN client works, including its main features.
- Chapter 2, “Installing the Cisco VPN 5000 Client.” This chapter describes how to install the VPN client software.
- Chapter 3, “Running the Cisco VPN 5000 Client.” This chapter describes how to operate the VPN client.
- Chapter 4, “Cisco VPN 5000 Client User Interface.” This chapter describes the windows and features of the VPN client.
- Appendix A, “Configuration File Keywords.” This appendix lists acceptable section names and keywords for editing the configuration file.
- Index

# Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

## World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

## Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

## Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

# Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

# Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

## Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

## Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

CHAPTER 1

# Introduction to the Cisco VPN 5000 Client

The Cisco VPN 5000 Client connects a remote user to a corporate network.

The user connects to a local Internet Service Provider (ISP). Then, using the VPN client, the user connects to the VPN concentrator Internet IP address to create a secure tunnel for passing IP packets between the remote user and the corporate network.

The VPN client encapsulates the data in a routable IP packet and encrypts it using the IP Security (IPSec) Protocol.

The corporate server or concentrator authenticates the user, decrypts and authenticates the IPSec packet, and translates the source address in the packets to an address recognized on the corporate network. This address is used for all traffic sent from the corporate network to the remote user for the duration of the connection.

## Features

The VPN client distinguishes between tunneled and nontunneled traffic and, depending on your concentrator configuration, allows simultaneous access to the corporate network and to Internet resources.

Cisco VPN 5000 Client software is available for the Macintosh operating system, Version 10.0, or Mac OS X.

The VPN client communicates over PPP links (including dialup and ISDN) and over Internet-attached Ethernet connections (including DSL and cable modem).

Table 1-1 describes the VPN client features.

***Table 1-1 VPN Client Features***

| Feature | Description |
|---|---|
| Operating systems | Mac OS X Version 10.0.0 to 10.1. |
| Connection types | • PPP, including dialup and ISDN<br>• Ethernet, including DSL and cable modem |
| Protocols | • IP |
| Tunnel protocol | IPSec |
| User authentication | • RADIUS<br>• RSA SecurID<br>• Axent Defender<br>• PKI user certificates (Entrust and RSA Security CAs only) |

CHAPTER 2

# Installing the Cisco VPN 5000 Client

This chapter describes how to install and uninstall the Cisco VPN 5000 Client on your computer for the Macintosh operating system Version 10.0, or Mac OS X.

You can obtain the install file by downloading it from the Cisco Systems website or from your network administrator. The VPN client install file is located in the VPN5000 folder.

## Contents

This chapter contains the following sections:


- Uninstalling the VPN Client for Mac OS X, page 2-1
- System Requirements, page 2-2
- Installing the Software, page 2-2


**Note** Before you install a new version of the VPN client for Mac OS X, you must first uninstall any earlier versions of the VPN client, and reboot your computer.

# Uninstalling the VPN Client for Mac OS X

To uninstall the VPN client for Mac OS X you must run the vpn_uninstall scripts located in the /Applications/VPN5000Client directory.

To uninstall the VPN client:

**Step 1** Log in as root user or superuser.

**Step 2** Make sure you are in the Applications/VPN5000 folder.

**Step 3** Enter the following command from a terminal window:

```
./vpn_uninstall
```

This method completely uninstalls all previous versions of the VPN client.

If running the uninstall script does not work, you can manually uninstall the VPN client by issuing the following set of commands from a terminal window as the root user or superuser:

```
rm -rf /Library/Receipts/vpn5000macosx510.pkg/
rm -rf /System/Library/Extensions/VPN5000.kext/
rm -rf /System/Library/StartupItems/VPN/
rm -rf /Applications/VPN5000Client/
```

**Step 4** Reboot your computer.

# System Requirements

The VPN client for Mac OS X runs on any Power Macintosh or compatible computer with the Macintosh operating system Versions 10.0.0 to 10.1.

Have available an application that can unpack the archive, such as StuffIt. This application is included with the VPN client. Your web browser might perform the translation automatically for you.

# Installing the Software

This section describes the installation process for the VPN client for Mac OS X. You must have root login priveleges for the computer on which you are installing the VPN client.

To install the VPN client for Mac OS X

**Step 1** From the VPN5000 folder, translate the set-up file from tar.gz using the StuffIt application.

This operation creates two files: a tar file and a pkg file.

**Step 2** If your tar.gz application did not expand the set-up package you must enter the following commands from a terminal window:

```
gunzip vpn5000-macosx-510-k9.tar.gz
tar -xvf vpn5000-macosx-510-k9.tar
```

This set of commands creates an installer package named vpn5000-macosx-510-k9.pkg.

**Step 3** In a Finder application window, double-click the vpn5000-macosx-510-k9.pkg icon and follow the instructions to install the VPN client.

**Step 4** Restart your computer.

After your computer completes the restart process, you can run the VPN client program.

CHAPTER 3

# Running the Cisco VPN 5000 Client

This chapter describes how to use the Cisco VPN 5000 Client for Mac OS X.

For an overview of the software user interface, see Chapter 4, "Cisco VPN 5000 Client User Interface."

## Contents

This chapter contains the following sections:


- Setting Up a Login, page 3-1
- Setting Up Digital Certificates, page 3-4
- Connecting to the VPN Concentrator, page 3-8
- Configuration File Description, page 3-9


## Setting Up a Login

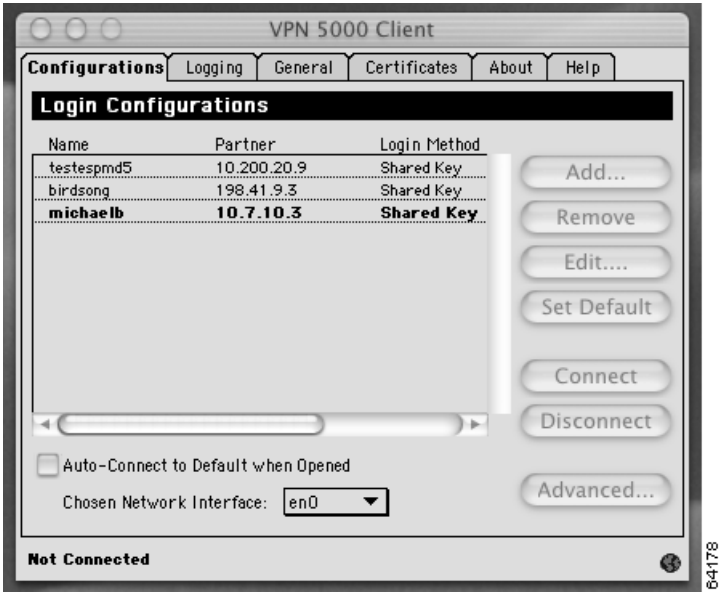
This section describes how to set up a login if your administrator has not already done so.

To set up your own login configuration

**Step 1** Double-click the VPN client icon on your desktop.

The VPN Client window opens with the Configurations tab forward (Figure 3-1).

***Figure 3-1 VPN Client Window***




**Step 2** Click the **Add** button.

The Login Properties dialog box opens.

**Step 3** Choose your login method.

If you choose Shared Secret, a shared key password authenticates the server during the login.

If you choose Certificate, a digital certificate is used for authentication during the login. Table 3-1 describes the digital certificate login methods.

*Table 3-1 Digital Certificate Login Methods*

| Certificate Type | Description |
|---|---|
| Manual | Manual login method—Uses a root certificate to validate the concentrator to the VPN client. See the "Manual Certificates" section on page 3-4 for more information. |
| User | User login method—Requires both a user certificate and a root certificate. The user certificate validates the VPN client user to the concentrator, and the root certificate validates the concentrator to the VPN client. See the "User Certificates" section on page 3-5 for more information. |

To add certificates after the initial login, see the "Certificates Tab" section on page 4-12.

**Step 4** Enter the login name assigned by your network administrator.

**Step 5** Enter the IP address or domain name of the VPN concentrator that you log in to.

You also have the option to set a secondary concentrator address, choose NAT transparency, and select your NAT port in this dialog box.

For information regarding other entry fields in the Login Properties dialog box, see the "Login Properties Dialog Box" section on page 4-5.

**Step 6** Click **OK**.

You are now back to the Configurations tab.

**Step 7** Select a network interface for the VPN client to use.

The network interface is applied to the VPN client software application and does not differ between users. For example, if you choose Ethernet 0 (en0), every connection attempt to a concentrator has the VPN client's network kernel extension attached to Ethernet 0.

**Step 8** Click **OK**.

**Step 9** Connect to the server as described in the "Connecting to the VPN Concentrator" section on page 3-8.

# Setting Up Digital Certificates

Digital certificates are special encrypted text files that are generated by a trusted Certificate Authority (CA). Certificates encrypt and decrypt your data, and replace the shared secret method for user and concentrator authentication.

The VPN client can be configured to use root (manual) certificates or user certificates. Root certificates authenticate the concentrator that you are connecting to. User certificates authenticate both the concentrator and the user.

Digital certificates can be obtained using any of the following methods:

- You can import certificates from another location using a browser window. This method is discussed in the following sections.
- You can request a root or user certificate from a CA using the Certificates tab of the VPN Client window. See the "Requesting Certificates from a Certificate Authority" section on page 3-7.

Manual and user certificates are defined in the configuration file for each user. For information on the configuration file, see the "Configuration File Description" section on page 3-9.

## Manual Certificates

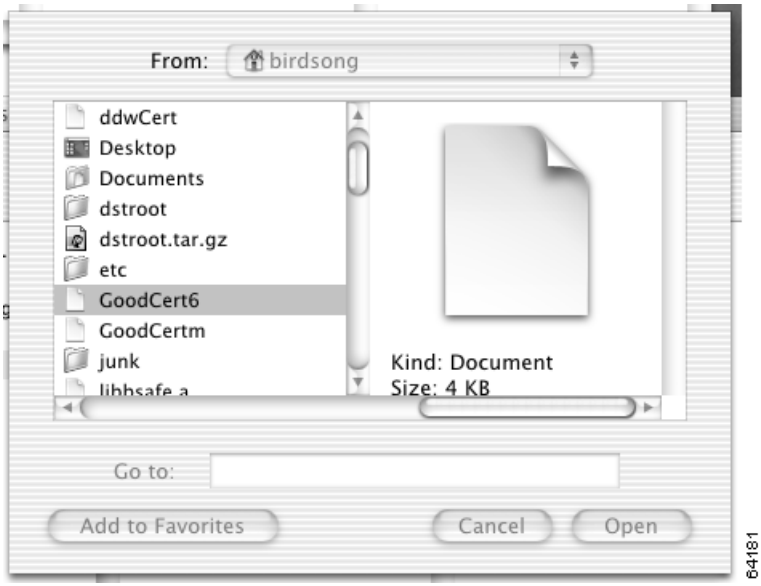
If you choose the manual login method, the system uses a root certificate to validate the concentrator to the VPN client.

Each VPN client uses a root certificate file, called rootcert, which is generated by the same CA that generated the concentrator's certificate. The root certificate identifies the CA to the client. All clients connecting to concentrators certified by the same CA use the same root certificate.

**Note** If one or more root certificate files are already defined in the configuration file, you are not prompted to select one.

If there are no root certificates in the configuration file, a file browser window (Figure 3-2) appears to allow you to import a root certificate file to be used during login.

***Figure 3-2 Import Root Certificate Window***




You can also access this window by clicking the **Import** button on the Certificates tab of the VPN Client window.

Each root certificate in the configuration file is validated during the login.

# User Certificates

The user login method requires both a user certificate and a root certificate. The user certificate validates the VPN client user to the concentrator, and the root certificate validates the concentrator to the VPN client. User certificates are associated with one user, while root certificates are associated to a concentrator and can be used by multiple users.

If there is no user certificate in the configuration file, a file browser window (Figure 3-2) appears to allow you to import a user certificate file to be used during login. A root certificate must exist in the configuration file; otherwise, you are prompted to import a root certificate using a file browser window as shown in Figure 3-3.

***Figure 3-3 Import Root Certificate Prompt***

**Note** If both the user and root certificate files are already defined in the configuration file, you are not prompted to select one.

You can also access this browser window by clicking the **Import** button on the Certificates tab of the VPN Client window.

When you exit the Login Properties dialog box, the root and user certificate files that you select are copied in the configuration file.

# Requesting Certificates from a Certificate Authority

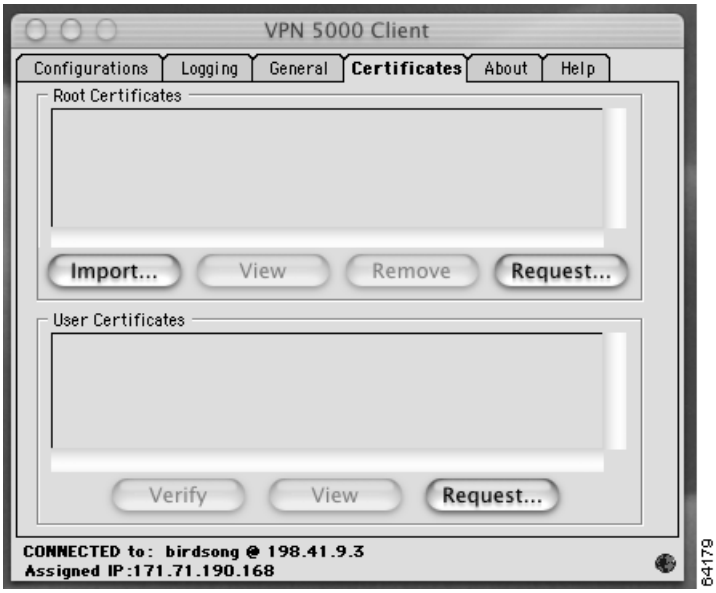
You can also request a user or root certificate from a CA.

- If you request a root certificate, the server script obtains a root certificate from the CA.
- If you request a user certificate, the server script obtains both a root and a user certificate from the CA.

To request a root or user certificate from a CA

**Step 1** Click the **Request** button on the Certificates tab of the VPN Client window (Figure 3-4).

***Figure 3-4 VPN Client Window—Certificates Tab***




- For root certificates, the Request Root Certificate dialog box appears.
- For user certificates, the Request User Certificate dialog box appears.

**Step 2** Enter the IP address and URL of the server script of the CA.

User certificates require you to enter both the root certificate request information and the user certificate request information.

For information on these entry fields, see the "Certificates Tab" section on page 4-12.

# Connecting to the VPN Concentrator

You can connect to a VPN concentrator after startup and login.

## Connecting After Startup and Login

To establish tunnel sessions after startup

**Step 1** Double-click the VPN client icon on your desktop.

The VPN Client window opens with the Configurations tab forward (see Figure 3-1).

**Step 2** Select a login name.

**Step 3** Click the **Connect** button.

**Tip** To automatically establish a tunnel session after startup, check the **Auto-Connect to Default when Opened** check box on the Configurations tab of the VPN Client window.

**Step 4** Respond to each security prompt. Your configuration might require you to respond to one or more of the following security prompts:

- Encryption Password
- Shared Secret
- RADIUS Login
- SecurID challenge

For more information on security prompts, see the "Security Prompts" section on page 4-20.

**Step 5** Click **OK**.

A successful connection is indicated by a black dot that appears next to the selected login name and a connection message appears at the bottom of the window.

**Note** When the VPN client is connected, all DNS traffic is tunneled as designated by the configuration in the concentrator. All other Internet traffic follows normal routing.

## Disconnecting the VPN Client

Choose any of the following methods to disconnect the VPN client:

- Click the Disconnect button on the Configurations tab of the VPN Client window. See Figure 4-1 on page 4-2.
- Press the keyboard combination "Apple-key" and Q simultaneously.
- In the VPN5000 menu, choose the Quit VPN5000 option. See Figure 4-18 on page 4-26.

# Configuration File Description

The configuration file contains information on passwords, security features, IP addresses, and connection protocols. A configuration file is automatically generated each time you exit the VPN client. The file is saved in the same folder in which the installer resides. See the "Example Configuration File" section on page A-5 for more information.

The name and location of the configuration file is VPN Client Preferences, and is located in the Preferences folder. Each user has their own Preferences folder. It is located in the Library folder of your home directory.

To edit the configuration file, refer to Appendix A, "Configuration File Keywords."

CHAPTER 4

# Cisco VPN 5000 Client User Interface

This chapter describes all of the windows, dialog boxes, and features of the Cisco VPN 5000 Client user interface.

## Contents

This chapter includes the following sections:


- VPN Client Window, page 4-1
  - Configurations Tab, page 4-2
  - Logging Tab, page 4-9
  - General Tab, page 4-11
  - Certificates Tab, page 4-12
  - About Tab, page 4-19
  - Help Tab, page 4-20
- Security Prompts, page 4-20
- File Menu, page 4-26


## VPN Client Window

To access the VPN Client window while you are connected, choose the VPN 5000 Client from the Finder menu. To quit, enter "**Apple-key"** and **Q** simultaneously.

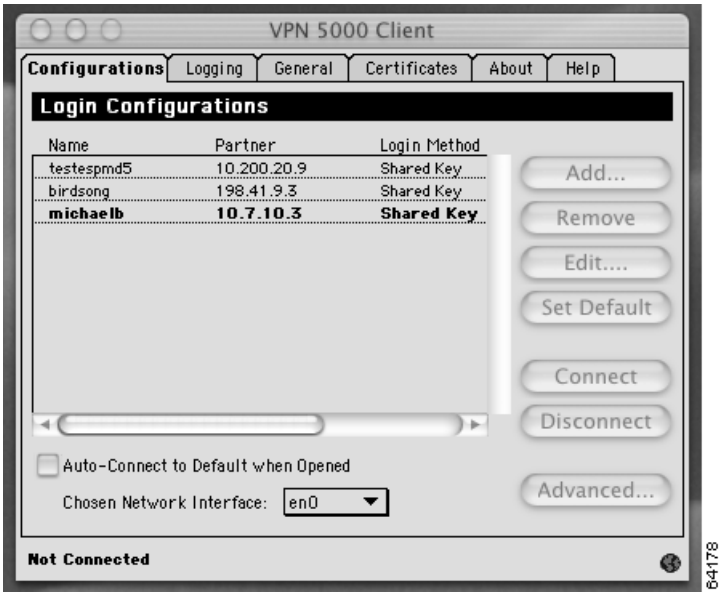
The following sections describe the different tabs on the VPN Client window. Use these windows to set up logins, view statistics, and set other VPN client parameters.

# Configurations Tab

The Configurations tab in the VPN Client window contains a list of possible login configurations. To establish a tunnel session, select the login configuration you want to use and click the **Connect** button.

Figure 4-1 shows the VPN Client window with the Configurations tab forward.

***Figure 4-1 Configurations Tab***




To add or modify existing login configurations, use the buttons described in Table 4-1. To set auto-connect preferences, see Table 4-2.

*Table 4-1 Configurations Tab Buttons*

| Button | Action |
|---|---|
| Add | Creates a new login configuration. |
| Remove | Deletes a login configuration. |
| Edit | Edits the selected login configuration. |
| Set Default | Sets a preselected login configuration when the client loads. |
| Connect | Establishes a tunnel connection using the selected login configuration. |
| Disconnect | Disconnects the active tunnel session. |
| Advanced | Opens the Advanced Configuration Properties dialog box. |

*Table 4-2 Configurations Tab Check Box*

| Check Box | Action |
|---|---|
| Auto-Connect to Default when Opened | Sets whether or not the default login configuration automatically connects to the concentrator when you open the VPN client. |

## Network Interface

When you open the VPN client application, a list of currently active network interfaces are displayed in a drop-down menu. For example, your VPN client might display the following network interfaces:

- en0, for an Ethernet card
- en1, for a wireless card
- ppp0, for a dialup connection

The first active interface detected upon startup is the default.

The network interface is applied to the VPN client software application and does not differ between users. For example, if you choose Ethernet 0 (en0), every connection attempt to a concentrator has the VPN client's network kernel extension attached to Ethernet 0.

You can only change the network interface when the VPN client is not connected to a concentrator. If you try to change the network interface while you have a connection established, you receive a warning message.

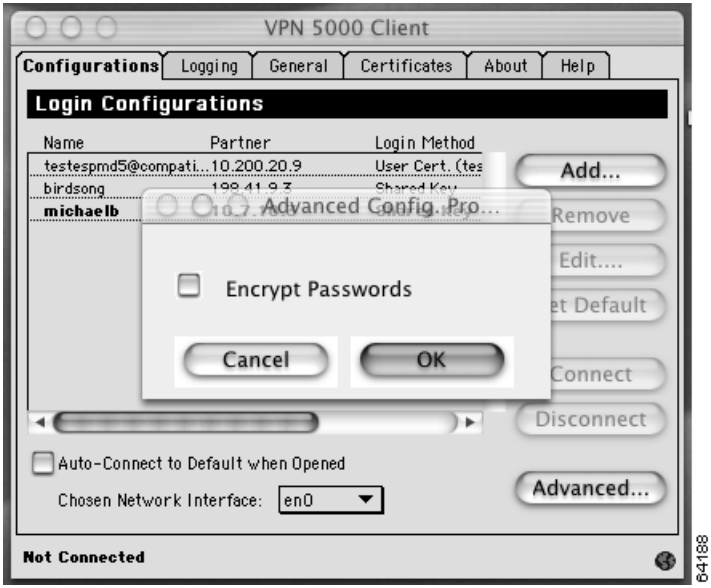
## Advanced Configuration Properties Dialog Box

If the concentrator is configured to save secrets, all static passwords entered in the VPN client are saved in the configuration file so you do not need to enter passwords again.

To prevent your passwords from being read in the configuration file, enable password encryption in the file by checking the Encrypt Passwords box on the Advanced Configuration Properties dialog box.

To access the Advanced Configuration Properties dialog box (Figure 4-2), click the **Advanced** button on the Configuration tab of the VPN Client window.

*Figure 4-2 Advanced Configuration Properties Dialog Box*




To disable password encryption

**Step 1** Uncheck the Encrypt Passwords box.

The VPN Client – VPN Encryption Password dialog box appears.

See the "VPN Client—VPN Encryption Password" section on page 4-21.

**Step 2** Enter your VPN encryption password.

**Step 3** Click **OK**.

**Step 4** In the Advanced Configuration Properties dialog box, click **OK**.

## Login Properties Dialog Box

The Login Properties dialog box allows you to enter and change parameters for the selected login configuration. To access this dialog box, click the **Add** or **Edit** button on the Configurations tab of the VPN Client window.

Many parameters require that the client be configured to match the configuration of the concentrator. For more information on configuring your concentrator, refer to the *Cisco VPN 5000 Concentrator Series Command Reference Guide* or the *Cisco VPN 5000 Concentrator Software Configuration Guide*.

Figure 4-3 shows the Login Properties dialog box, and Table 4-3 describes the entry fields.

***Figure 4-3 Login Properties Dialog Box***

*Table 4-3 Login Properties Dialog Box Entry Fields*

| Parameter | Description |
|---|---|
| Shared Key | This login method uses only the shared key password for authentication. |
| Certificate | If you select the Certificate radio button, a drop-down menu appears to allow you to choose your certificate type.<br>If you choose:<br>• Manual—Specifies that a root certificate is used for authentication during the login. If no root certificate is defined in the configuration file, you can import one using the Import Root Certificate browser window, or request one from the CA using the Request Root Certificate dialog box.<br>• User—Specifies that both a root certificate and a user certificate are used for authentication during the login. If no user certificate is defined in the configuration file, you can import one using the Import User Certificate browser window, or request one from a CA using the Request User Certificate dialog box. |
| Login Name | Name of the tunnel user. This name must also be configured either on the concentrator or, if present, an authentication server. The name can be between 1 and 60 alphanumeric characters (no spaces allowed). |
| Primary VPN Server | IP address or fully qualified domain name of the concentrator that the VPN client software connects to. Domain names can be up to 80 characters. |

*Table 4-3 Login Properties Dialog Box Entry Fields (continued)*

| Parameter | Description |
|---|---|
| Secondary Server | Alternate concentrator address. |
| Use NAT Transparency Mode | Enables Network Address Translation (NAT) transparency for client sessions. The concentrator must be configured to have an ESP transform set. Check Use NAT Transparency if you are having problems connecting through a NAT device or through an ISP. |
| NAT Port | This feature allows you to set the destination TCP port for outgoing VPN packets.<br>The NAT port on the VPN 5000 client must match the port number that is configured in **NATTransport** keyword in the **General** section on the concentrator.<br>The value can be between 0 and 65536. The default is 80. |
| Advanced button | Opens the Advanced Login Properties dialog box. |

## Advanced Login Properties Dialog Box

The Advanced Login Properties dialog box sets local tunneling control. To access this dialog box, click the **Advanced** button on the Login Properties dialog box. Figure 4-4 shows the Advanced Login Properties dialog box, and Table 4-4 describes each parameter.

*Figure 4-4 Advanced Login Properties Dialog Box*

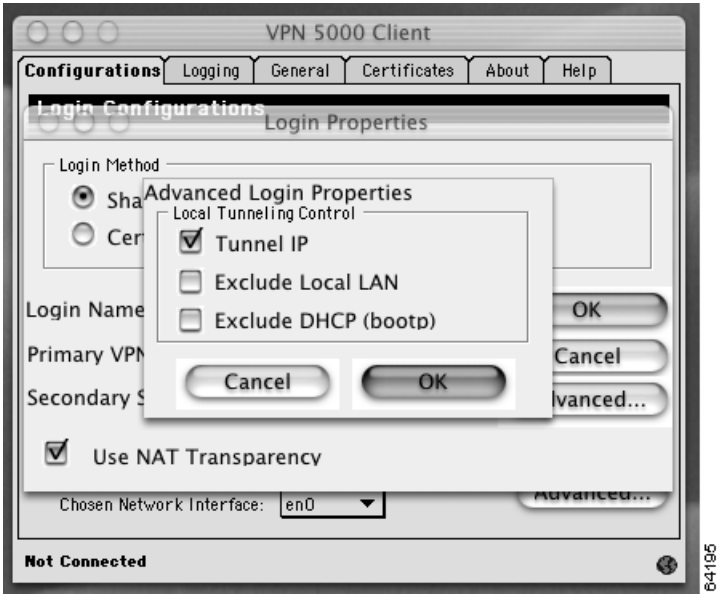


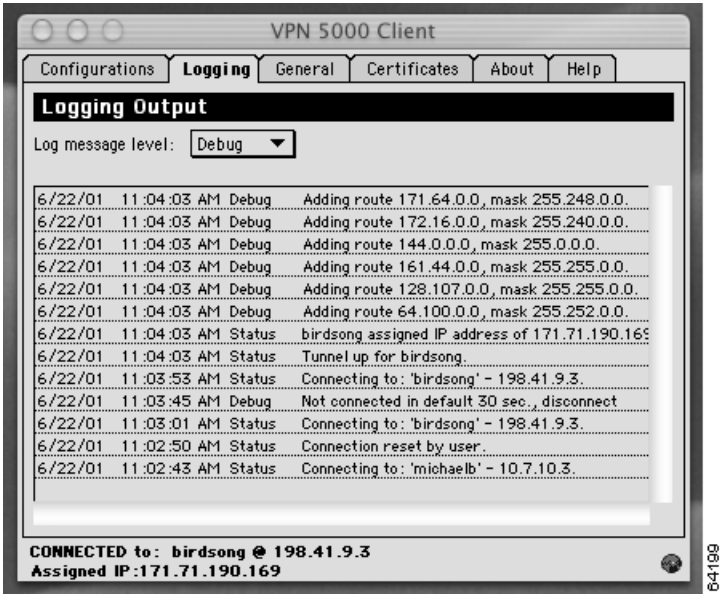

*Table 4-4 Advanced Login Properties Dialog Box Parameters*

| Check Box | Action |
|---|---|
| Tunnel IP | Enables IP-in-IP tunneling to the IP networks configured in the concentrator. |
| Exclude Local LAN | Local LAN traffic (for the directly connected network only) is not tunneled, if enabled on the concentrator. |
| Exclude DHCP (bootp) | DHCP traffic is not tunneled. |

# Logging Tab

The Logging tab displays messages related to tunnel connections for troubleshooting purposes (Figure 4-5).

*Figure 4-5 Logging Tab*


VPN 5000 Client
Configurations
Logging
General
Certificates
About
Help
Logging Output
Log message level:
Debug
6/22/01 11:04:03 AM Debug Adding route 171.64.0.0, mask 255.248.0.0.
6/22/01 11:04:03 AM Debug Adding route 172.16.0.0, mask 255.240.0.0.
6/22/01 11:04:03 AM Debug Adding route 144.0.0.0, mask 255.0.0.0.
6/22/01 11:04:03 AM Debug Adding route 161.44.0.0, mask 255.255.0.0.
6/22/01 11:04:03 AM Debug Adding route 128.107.0.0, mask 255.255.0.0.
6/22/01 11:04:03 AM Debug Adding route 64.100.0.0, mask 255.252.0.0.
6/22/01 11:04:03 AM Status birdsong assigned IP address of 171.71.190.169
6/22/01 11:04:03 AM Status Tunnel up for birdsong.
6/22/01 11:03:53 AM Status Connecting to: 'birdsong' - 198.41.9.3.
6/22/01 11:03:45 AM Debug Not connected in default 30 sec., disconnect
6/22/01 11:03:01 AM Status Connecting to: 'birdsong' - 198.41.9.3.
6/22/01 11:02:50 AM Status Connection reset by user.
6/22/01 11:02:43 AM Status Connecting to: 'michaelb' - 10.7.10.3.
CONNECTED to: birdsong @ 198.41.9.3
Assigned IP:171.71.190.169
64199

The Log message level drop-down list determines the detail of messages logged. The log information is displayed in the window. Table 4-5 describes the levels of log messages.

*Table 4-5 Log Message Level Options*

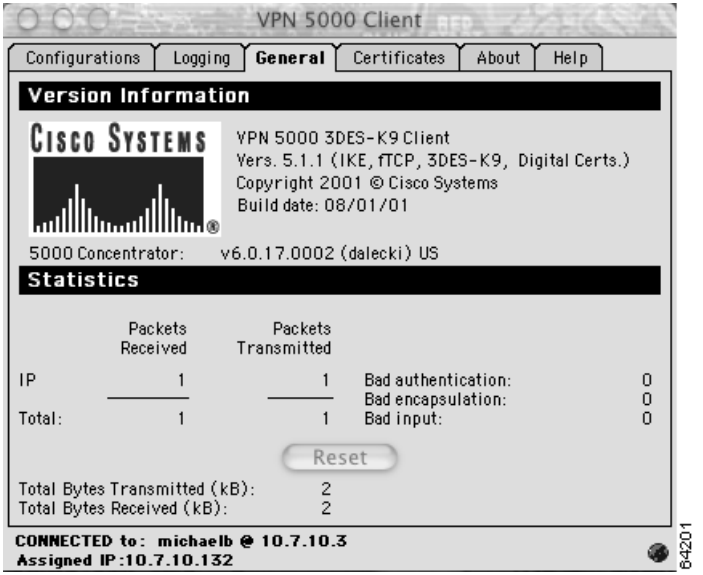
| Log Message Level | Description |
|---|---|
| Error | Reports errors. |
| Warning | Reports warnings and errors. |
| Status | Reports connection status, warnings, and errors. |
| Debug | Reports every action and provides detailed information about the connection conversation between the client and the concentrator. |

**Caution** We recommend that you do not use Debug on a daily basis. It generates a large number of log messages.

# General Tab

The General tab displays information about the VPN client and packet statistics for each session (Figure 4-6).

***Figure 4-6 General Tab***




The Version Information section displays the current version of the VPN client software, copyright information, software build date, and the version number of the code for the last VPN 5000 concentrator the VPN client was connected to.

The IP address the VPN 5000 concentrator gives to the VPN client for this session is displayed at the bottom of the VPN Client window.

The Statistics section displays information related to tunnel traffic (Table 4-6). This information is used for troubleshooting purposes.

*Table 4-6 General Statistics*

| Statistics Field | Description |
|---|---|
| Packets Received and Packets Transmitted | Number of IP and IPX packets received and transmitted by the client during the active session. |
| Bad authentication | Number of packets with bad authentication. A bad authentication error means that the check on the digital signature failed. |
| Bad encapsulation | Number of packets with bad encapsulation. A bad encapsulation error usually means that the packet headers could not be found. |
| Bad input | Number of packets that could not wrap properly. |
| **Statistics Field** | **Description** |
| Bytes Received and Bytes Transmitted | Can be used for billing purposes. These fields list the number of bytes transmitted and received by the client during the active session. |
| Reset | Clears all displayed statistics except bytes received and transmitted. |

# Certificates Tab

The Certificates tab allows you to manage your root and user certificates.

During the login:

- Each *root* certificate file is checked against the received concentrator certificate for validity until the concentrator's certificate is validated, or until there are no more root certificates. Root certificates are not bound to any user.
- Each *user* certificate is associated with a particular root certificate. During the login, each user certificate is checked against each root certificate for validation. User certificates are bound to the user.

Figure 4-7 shows the Certificates tab of the VPN Client window and Table 4-7 describes each button.

*Figure 4-7 Certificates Tab*

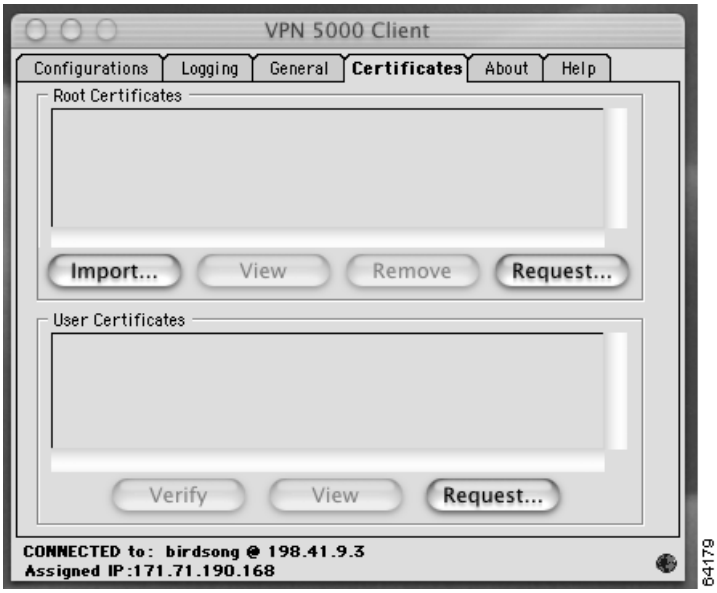



*Table 4-7 Certificates Tab Buttons*

| Button | Action |
|---|---|
| Import | Imports root certificates. |
| Remove | Removes unused or unneeded root certificates. |
| Verify | Verifies that the selected user certificate includes an associated root certificate. |
| View | Opens the Digital Certificate Information window (Figure 4-10). |
| Request | For root certificates, this button opens the Request Root Certificate dialog box (Figure 4-8). For user certificates, this button opens the Request User Certificate dialog box (Figure 4-9). |

## Request Root Certificate Dialog Box

The Request Root Certificate dialog box (Figure 4-8) appears if you request your root certificate from a CA. See the "Requesting Certificates from a Certificate Authority" section on page 3-7 for more information.

***Figure 4-8 Request Root Certificate Dialog Box***

Table 4-8 describes the entry fields for the Request Root Certificate dialog box.

***Table 4-8 Request Root Certificate Entry Fields***

| Parameter | Description |
|---|---|
| IP Address | IP address of the CA. |
| URL | Location of the scep server script. |

## Request User Certificate Dialog Box

The Request User Certificate dialog box (Figure 4-9) appears if you request a user certificate from a CA. A request for a user certificate requires both root certificate information and user certificate information.

***Figure 4-9 Request User Certificate Dialog Box***

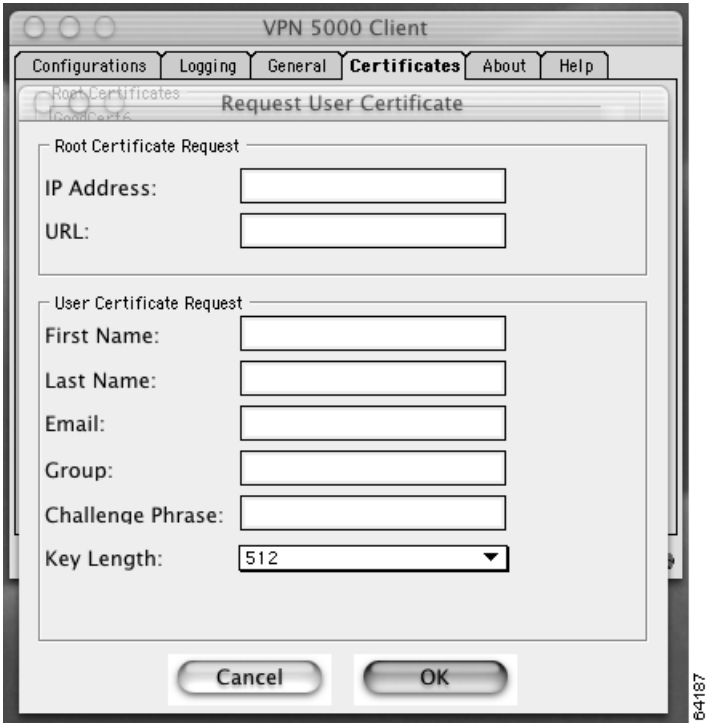



Table 4-9 describes the entry fields in this dialog box.

***Table 4-9 Request User Certificate Entry Fields***

| Parameter | Description |
|---|---|
| First Name | User's first name. |
| Last Name | User's last name. |

*Table 4-9 Request User Certificate Entry Fields (continued)*

| Parameter | Description |
|---|---|
| Email | User's e-mail address. |
| Group | VPN group on the concentrator. |
| Challenge Phrase | Password used to validate the user to the network administrator. |
| Key Length | Valid key length of the user certificate. |

## Digital Certificate Information Window

The Digital Certificate Information window (Figure 4-10) displays details about the selected root or user certificate. To access this window, click either of the **View** buttons on the Certificates tab of the VPN Client window. Table 4-10 provides a description of each field in the Digital Certificate Information window.

*Figure 4-10 Digital Certificate Information Window*

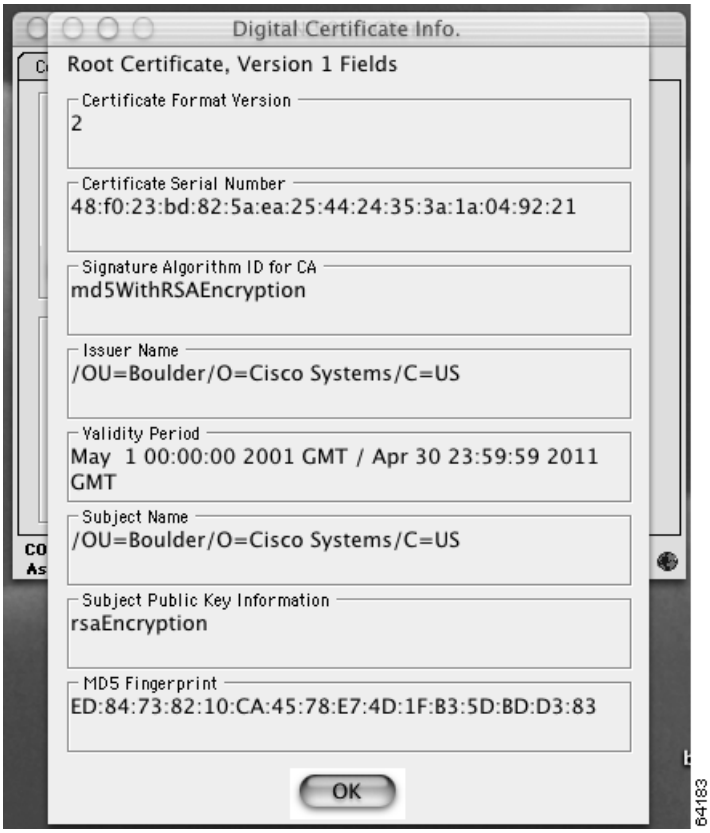



*Table 4-10 Digital Certificate Information Fields*

| Field | Description |
|---|---|
| Certificate Format Version | Indicates the X.509 version of the certificate format. |
| Certificate Serial Number | Specifies the unique numerical identifier of the certificate in the domain of all public key certificates issued by the CA. |
| Signature Algorithm ID for CA | Identifies the algorithm used by the CA to sign the certificate. |

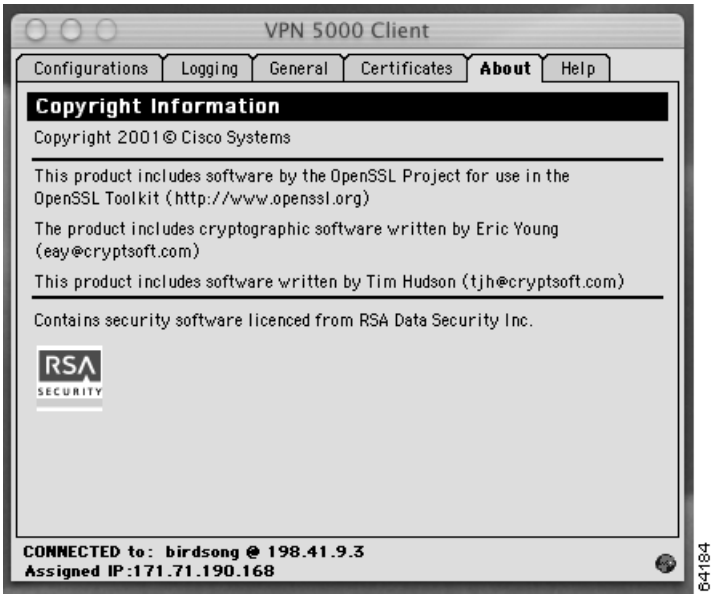
*Table 4-10 Digital Certificate Information Fields (continued)*

| Field | Description |
|---|---|
| Issuer Name | Specifies the X.500 distinguished name (DN) of the CA that issued the certificate. |
| Validity Period | Specifies the start dates and times, and the expiration date of the certificate. |
| Subject Name | Specifies the X.500 DN of the entity holding the private key corresponding to the public key identified in the certificate. |
| Subject Public Key Information | The first part of this field identifies the value of the public key owned by the subject. The second part is the algorithm identifier specifying the algorithm with which the public key is to be used. |
| MD5 Fingerprint | Identifies the fingerprint of the certificate so that it can be verified against the certificate on the concentrator. |

# About Tab

The About tab of the VPN Client window displays product licensing and copyright information (Figure 4-11).

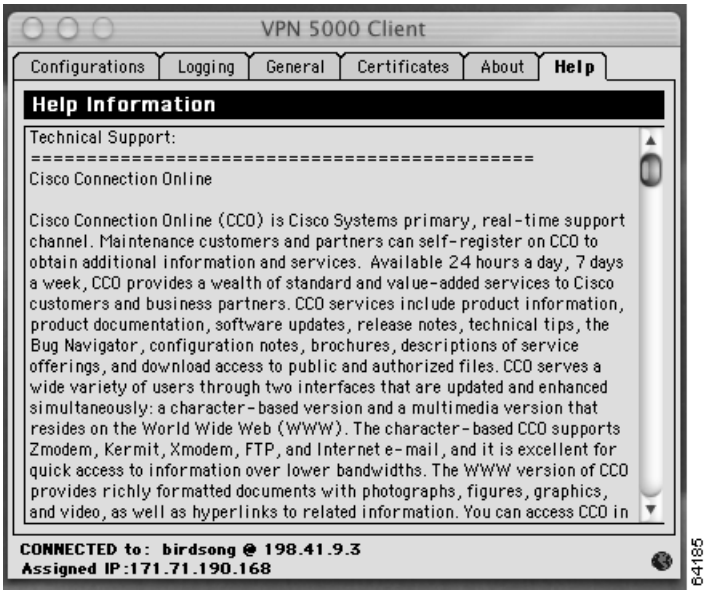
***Figure 4-11 About Tab***



# Help Tab

The VPN client for Mac OS X includes a help file with a Help tab on the VPN Client window (Figure 4-12).

***Figure 4-12 Help Tab***


VPN 5000 Client
Configurations
Logging
General
Certificates
About
Help
Help Information
Technical Support:
==========
Cisco Connection Online
Cisco Connection Online (CCO) is Cisco Systems primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services. Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files. CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information. You can access CCO in
CONNECTED to: birdsong @ 198.41.9.3
Assigned IP:171.71.190.168
64185

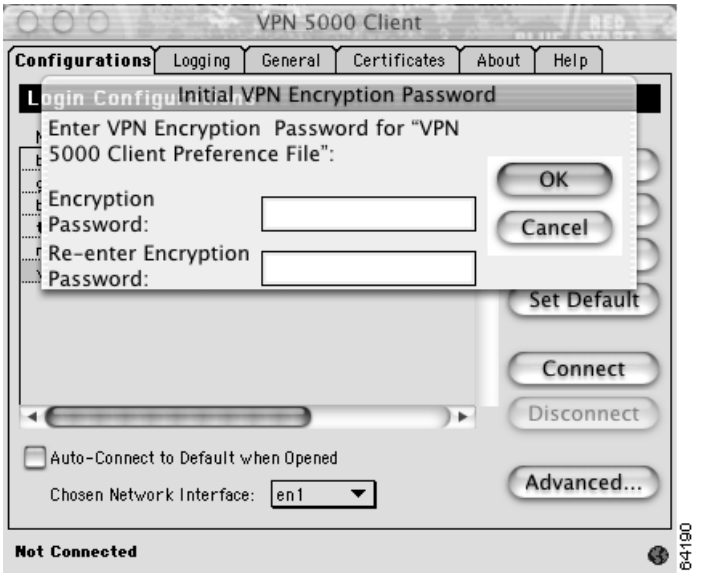
# Security Prompts

This section describes the security windows and dialog boxes that can appear during the login. The security prompts that appear depend on your configuration.

# VPN Encryption Password

The following dialog box (Figure 4-13) appears if you enabled password encryption to decrypt the passwords in your configuration file for tunnel session (see the "Advanced Configuration Properties Dialog Box" section on page 4-4).

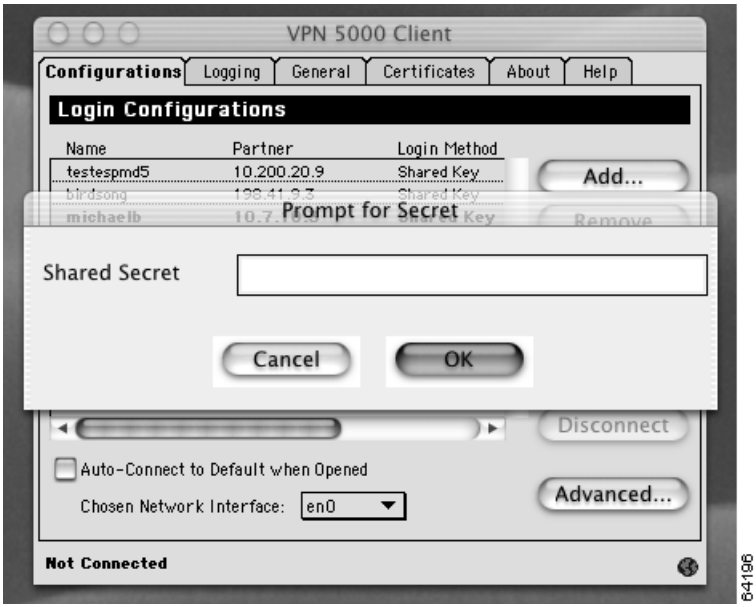
***Figure 4-13 VPN Client—VPN Encryption Password***




# Prompt for Secret

If you are not using certificates, you are prompted for a shared secret to establish a tunnel between the client and the concentrator (Figure 4-14). Additional passwords are sent over the tunnel. A shared secret is provided by your administrator.

*Figure 4-14 Prompt for Secret*



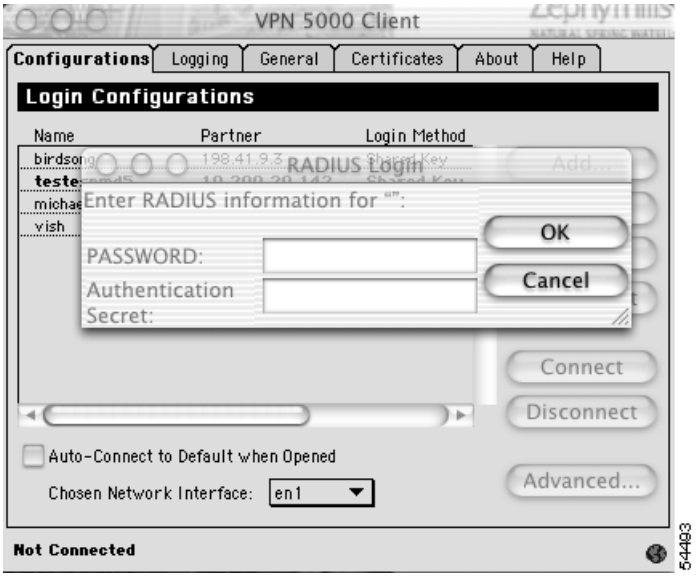

# RADIUS Login

If the VPN concentrator uses a RADIUS server to authenticate users, the RADIUS password and authentication secret verify the client to connect to the RADIUS VPN concentrator.

If the concentrator specifies PAP authentication, you are prompted by the dialog box shown in Figure 4-15.

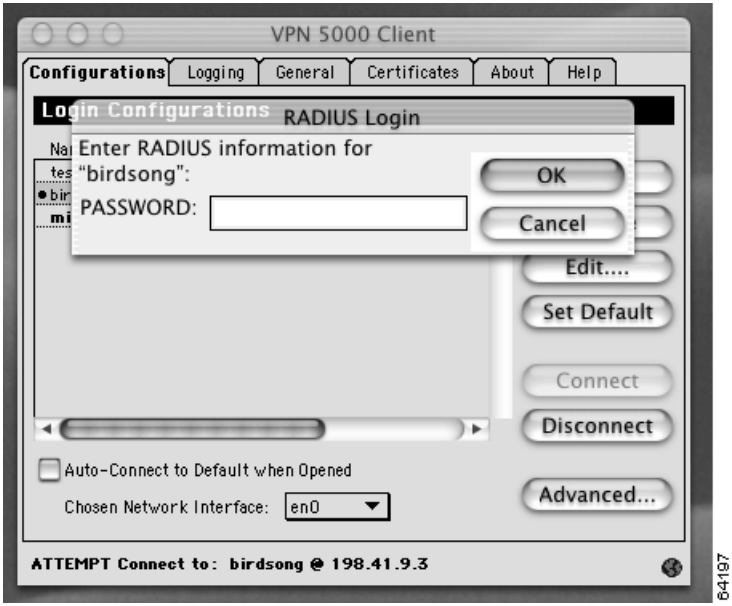
Enter the password and authentication secret in the RADIUS Login dialog box. The password is the RADIUS password configured on the RADIUS server. The authentication secret must match the PAPAuthSecret configured in the RADIUS section of the concentrator.

***Figure 4-15 RADIUS Login/PAP Dialog Box***



If the concentrator specifies CHAP authentication, you are prompted by the dialog box shown in Figure 4-16.

***Figure 4-16 RADIUS Login/CHAP Dialog Box***



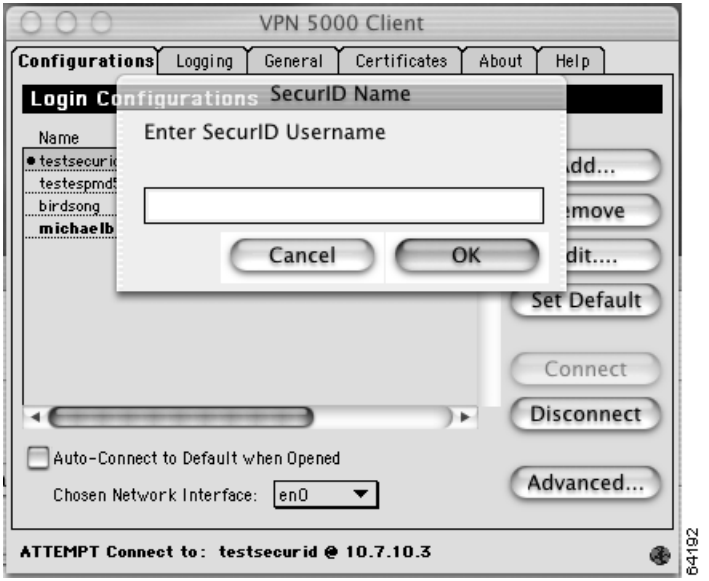

Enter the password in the VPN Client – RADIUS Password dialog box. The password is issued by the administrator.

# SecurID Challenge

Client configurations that use SecurID display several special user prompts. In some cases, all of the prompts described in this section appear. In other cases, only some of the prompts described appear.

If the concentrator configuration specifies that the SecurID user name is different from the concentrator login name, the VPN Client – SecurID Challenge dialog box appears (Figure 4-17).

*Figure 4-17 VPN Client—SecurID Challenge*




If the SecurID server is configured to require a PIN change, the first time you log in, the VPN Client – SecurID Challenge dialog box prompts you to change your PIN.

To change your PIN the first time you log in

**Step 1** Enter a PIN and click **OK**, or leave the edit box blank and click **Cancel** to make the system generate a PIN.

If the system generates the PIN, a window containing a new PIN appears.

Memorize or note the PIN before you click **OK**.

**Step 2** If you have logged in before, enter your SecurID passcode in the VPN Client – SecurID Challenge dialog box. The passcode consists of your PIN plus the current code from your SecurID token.

If the passcode is accepted, a client tunnel is created and the globe icon in the upper right corner of the VPN Client window starts spinning.

If the passcode is not accepted, you get an authentication failed message.

**Step 3** Wait until the token passcode changes from the passcode you just entered, and try again.

If the passcode is still unacceptable, an access denied message appears.

## Changing the SecurID Passcode

The administrator can set the SecurID server to require users to change their PINs.

To change your PIN at the request of the administrator

**Step 1** Enter a PIN in the VPN Client – SecurID Challenge dialog box, and click **OK**, or leave the edit box blank and click **Cancel** to make the system generate a PIN.

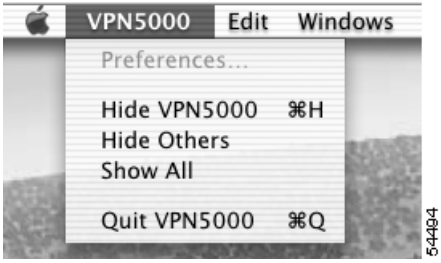
**Step 2** After memorizing or noting your new PIN, click **OK**.

**Step 3** Enter your new passcode and click **OK**.

# File Menu

The File menu (Figure 4-18) includes Hide, Show, and Quit commands.

***Figure 4-18 File Menu***




- To hide the VPN Client window, choose **Hide VPN5000**.
- To exit the program, choose **Quit VPN5000**.

APPENDIX A

# Configuration File Keywords

The configuration file has four valid section names:

- [VPN Partner Aliases]
- [VPN User]
- [VPN General Section]
- [VPN Root Cert]

The section names are not case sensitive.

# VPN Partner Aliases

Use the keywords listed in Table A-1 for aliasing VPN client IP addresses to a text string. **Alias_Name** is case sensitive.

***Table A-1 VPN Partner Aliases Keyword***

| Keyword | Description |
|---|---|
| **Alias_Name =** *IP_Address* | **Alias_Name** is any text string including spaces less than 80 characters. The *IP_Address* is a valid IP address of a VPN 5000 concentrator to which the client can connect. The IP address must be in standard dotted decimal format and not a domain name. |

# VPN User

Use the keywords listed in Table A-2 to manually define the login information for each user of the VPN client. There may be multiple users for each configuration file.

*Table A-2 VPN User Section Keywords*

| Keyword | Description |
|---|---|
| **UserName** = *string* | Identifies a unique user. This must be the same as the user name configured in the authentication service you are using (for example, RADIUS or SecurID). The string can be between 1 and 60 alphanumeric characters in length, with no spaces allowed. This entry must always be the first one on the line. |
| **IPPrimary** = {*Alias_Name* \| *IP_address* \| *Domain_Name*} | Sets the alias name, IP address, or fully qualified domain name of the VPN 5000 concentrator to which the client connects. |
| **IPSecondary** = {*Alias_Name* \| *IP_address* \| *Domain_Name*} | Sets the alias name, IP address, or fully qualified domain name of the VPN 5000 concentrator to which the client connects, if the primary concentrator is unreachable. |
| **SharedKey** = *pass_phrase* | Sets the shared secret for this user. The pass phrase generates session keys used to authenticate and encrypt each packet received from or sent to the client. This keyword must match the Shared Key configured for this user in the VPN authentication system. Save Secrets must also be enabled on the concentrator. |
| **RADIUSPassword** = *string* | Sets the **RADIUSPassword** keyword to match the user's password configured in the RADIUS server. Save Secrets must also be enabled on the concentrator. |

*Table A-2 VPN User Section Keywords (continued)*

| Keyword | Description |
|---|---|
| **PAPAuthSecret =** *pass_phrase* | Sets the secret used between the VPN 5000 concentrator and the client. This secret authenticates and encrypts packets exchanged before passing them on to the RADIUS server. Use this keyword if the RADIUS server is set to use PAP for authentication instead of CHAP. The **PAPAuthSecret** must match the secret configured in the RADIUS section of the VPN 5000 concentrator. Save Secrets must also be enabled on the concentrator. |
| **IPEnabled =** {**True** \| **False**} | When the **IPEnabled** keyword is true, the VPN client enables IP-in-IP tunneling to the corporate network. |
| **ExcludeLocalLAN =** {**True** \| **False**} | When the **ExcludeLocalLAN** keyword is true, local LAN traffic is not tunneled. You must also enable the **ExcludeLocalLAN** keyword in the VPN Group configuration of the VPN 5000 concentrator. |
| **ExcludeDHCP =** **{True \| False}** | When the **ExcludeDHCP** keyword is true, DHCP traffic is not tunneled. |
| **UsefTCP =** {**True** \| **False**} | When the **UsefTCP** keyword is true, you enable Network Address Translation (NAT) transparency for client sessions. Set this keyword if you experience a problem connecting through a NAT device or through an ISP. |
| **FTCPDestinationPort** = *Number* | Sets the NAT port you want to use.<br>The value can be between 0 and 65536. The default is 80. If you leave this value blank or specify a value outside the valid range, the value of 80 is assumed by the VPN client.<br>This port must match the number set in the **NATTransport** keyword in the **General** section for the concentrator. |

*Table A-2 VPN User Section Keywords (continued)*

| Keyword | Description |
|---|---|
| **LoginMethod** = **Entrust \| User \| Manual** | Sets the login method. Refer to Table 3-1 on page 3-3 for a description of each login method. |
| **UserCertLocation** = *string* | Name of the user certificate that is located in the IntraPort Client/certificates/user folder. |

# VPN General Section

Use the keyword listed in Table A-3 for setting general operations of the VPN client. These settings affect each user in the configuration file. Currently, the password encryption operation is on a per-user basis.

*Table A-3 VPN General Section Keyword*

| Keyword | Description |
|---|---|
| **EncryptPasswords** = {**True** \| **False**} | When the **EncryptPasswords** keyword is true, all pass phrases (**SharedKey**, **RADIUSPassword**, and **PAPAuthSecret**) are encrypted for every user in the configuration file. The user is prompted for the encryption password during the login. |

# VPN Root Cert

Use the keyword in Table A-4 for root certificates that were imported into the VPN client. Only one root certificate is allowed per section, but there may be as many as 30 VPN Root Cert sections.

*Table A-4 VPN Root Cert Section Keyword*

| Keyword | Description |
|---|---|
| **CertName** = *root_certificate_file_name* | Specifies the file name for each root certificate that was imported. |

Each root certificate must have its own section header as shown in the following examples:

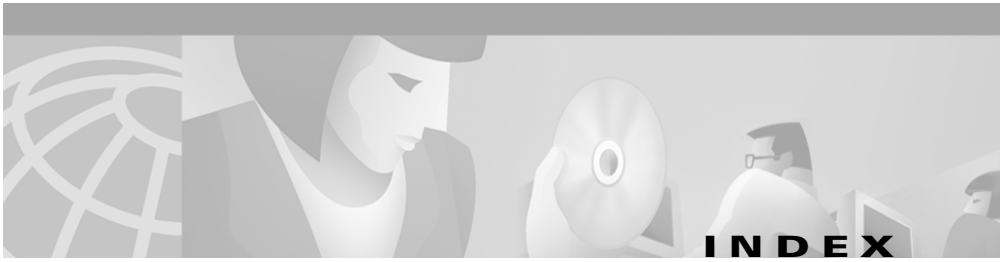
```
[VPN Root Cert]
CertName = rootcert_1

[VPN Root Cert]
CertName = rootcert_2
```

# Example Configuration File

This section shows an example configuration file.

```
[VPN General Section]

[VPN Partner Aliases]

[VPN Root Cert]
CertName = keonroot.txt

[VPN User]
UserName = zulu
IPPrimary = 1.0.0.0
IPSecondary =
SharedKey =
RADIUSPassword =
PAPAuthSecret =
IPEnabled = 1
IPXEnabled = 1
NetBTEnabled = 1
ExcludeLocalLAN = 0
ExcludeDHCP = 0
UseFTCP = 0
RXBytes = 0
TXBytes = 0
LoginMethod = Shared Key

[VPN User]
UserName = John@whatever.com
IPPrimary = 1.1.1.1
IPSecondary =
SharedKey =
RADIUSPassword =
PAPAuthSecret =
IPEnabled = 1
```

```
IPXEnabled = 1
NetBTEnabled = 1
ExcludeLocalLAN = 0
ExcludeDHCP = 0
UseFTCP = 0
RXBytes = 0
TXBytes = 0
LoginMethod = User
UserCertLocation = my12.p12
```




## A

About tab **4-19**
Advanced Configuration Properties dialog box **4-4**
aliasing client IP address **A-1**
authentication
  RADIUS login **4-22**
  supported **1-2**

## C

cable modem **1-2**
certificate requests
  root **4-14**
  user **4-15**
certificates
  managing **4-12**
  parameter for login **4-7**
  root
    generated **3-4**
    importing **3-4**
    selecting **4-7**
  user
    importing **3-5**
    selecting **3-3**
Certificates tab **4-12**
configuration file
  description **3-9**
  keywords **A-1 to A-5**
Configurations tab description **4-2**
connecting to the server
  after startup **3-8**
connection types **1-2**

## D

DHCP, excluding **4-9**
digital certificates **3-4**
DSL **1-2**

## E

Ethernet **1-2**
excluding DHCP traffic **4-9**

## F

File menu, Mac OS **4-26**

## G

General tab
  description **4-11**

## H

Help tab **4-20**

## I

importing root certificates **3-5**
IP
  support for **1-2**
  tunneling **4-9**
IPSec **1-2**
ISDN **1-2**

## K

keywords, configuration file **A-1**

## L

local LAN, excluding **4-9**
Logging tab **4-9**
login
  creating **3-2**
  parameters in **4-5**
Login Properties dialog box
  advanced properties **4-8**
  description **4-5**

## N

NAT Transparency mode **4-8**

## O

operating systems **1-2**
overview **1-1**

## P

packet statistics **4-12**
passcodes
  changing **4-26**
  SecurID **4-25**
passwords, encrypting **4-4**
PIN, changing **4-25**
PPP links **1-2**
Prompt for Secret **4-21**
protocols **1-2**

## R

RADIUS Login **4-22**
requesting a root certificate **4-14**

requesting a user certificate **4-15**

## S

secrets, encrypting **4-4**
section names
  VPN General **A-4**
  VPN Partner Aliases **A-1**
  VPN Root Cert **A-4**
  VPN User **A-2**
SecurID **4-24**
setting up a login **3-1**
shared key login **4-7**
software features **1-1**
statistics, tunnel traffic **4-12**
StuffIt **2-2**

## T

Tunnel protocols **1-2**
tunnels, establishing **3-8**

## U

uninstalling
  client **2-1**
user authentication
  specifying **3-3**
  supported **1-2**
user certificates, see certificates
user interface **4-1**

## V

VPN 5000 concentrator
  connecting to **3-8**
  specifying **3-3**
VPN Client window **4-1 to ??**
VPN Encryption Password **4-21**
VPN General section name **A-4**
VPN Partner Aliases section name **A-1**
VPN Root Cert section name **A-4**
VPN User section name **A-2**